(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
20 September 2001 (20.09.2001)

PCT

(10) International Publication Number
WO 01/69864 A2

(51) International Patent Classification[7]: H04L 12/56

(21) International Application Number: PCT/CA01/00288

(22) International Filing Date: 9 March 2001 (09.03.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/526,503 16 March 2000 (16.03.2000) US

(71) Applicant *(for all designated States except US)*: **TELEFONAKTIEBOLAGET LM ERICSSON (PUBL)** [SE/SE]; S-126 25 Stockholm (SE).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: **SAWYER, Francois** [CA/CA]; 1895 Megantic, St-Hubert, Québec J3Y 7H7 (CA). **STÅHL, Niclas** [SE/CA]; 525, rue Lucien L'Allier, apt. 101, Montreal, Québec H3C 4L3 (CA).

(74) Agents: **BEAUCHESNE, Sandra** et al.; Ericsson Canada Inc., 8400 Decarie Boulevard, Town of Mount Royal, Québec H4P 2N2 (CA).

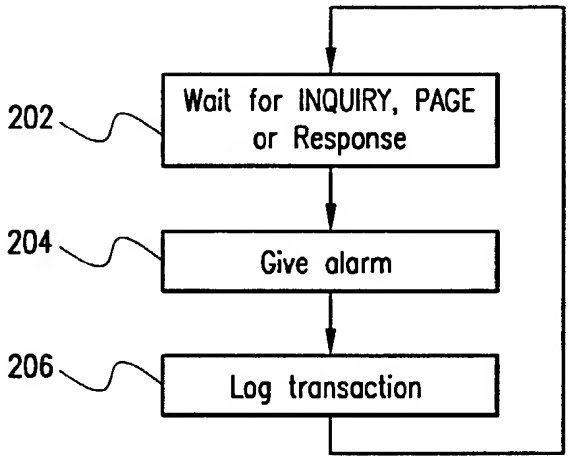
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

**Published:**
— *without international search report and to be republished upon receipt of that report*

*For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.*

(54) Title: METHOD AND APPARATUS FOR DETECTING BLUETOOTH COMMUNICATIONS




(57) Abstract: The present invention refers to a method and an apparatus for detecting Bluetooth transactions. The apparatus (20) comprises an antenna part (22) that is tuned to all possible Bluetooth carriers, a processor (24) that listens (step 202) for INQUIRY, PAGE and Response messages. When the processor detects any of above-mentioned messages it displays an alarm notice (step 204) on a display (28) and logs the information displayed (step 206) in a memory (26).

WO 01/69864 A2

# METHOD AND APPARATUS FOR DETECTING BLUETOOTH COMMUNICATIONS

## BACKGROUND OF THE INVENTION

### Technical Field of the Invention

The present invention relates to radio communication and, more specifically to an apparatus and a method for detection of Bluetooth transactions.

### Description of the Related Art

The advancements of radio communication have provided technologies that allow short-range radio communication between various devices. Examples of this are a wireless radio connection between a headset and a telephone and a wireless radio connection between a mobile telephone and a computer; the possibilities are almost limitless.

While these possibilities are desirable on most occasions, there are situations where they create problems. Imagine for example the following scenario:

Students at a university exam have brought their calculators, electronic organisers, portable computers and the like; everything equipped with short-range radio communication devices. Anyone in the room will then be able to communicate with everyone else in the room, discussing solutions and answers, or maybe even accessing the Internet. Such usage of short-range radio communication devices could not be detected by invigilators, and could affect students' results.

There are of course other situations where unauthorised communication is undesirable, for instance on airplanes; the exam situation being just an example.

Bluetooth, a technology well known to a person skilled in the art, makes this short-range interconnection possible. Some relevant features provided by Bluetooth are:

- strong encryption, needed for many applications, for example e-commerce, and
- fast frequency hopping.

The strong encryption makes it unfeasible to decrypt communication to find out what was sent – i.e. to decode ongoing communication, while the frequency hopping makes it very difficult or impossible to jam Bluetooth communication.

All in all, it can be appreciated that devices equipped with Bluetooth technology, while usually beneficial, sometimes cause problems.

Based on the foregoing, it can be readily appreciated that there is a need for a simple, efficient solution to the problem of how to detect Bluetooth communication as mentioned above. The present invention provides a solution to this problem.

## SUMMARY OF THE INVENTION

In one aspect, the present invention is directed to several embodiments of an apparatus for detecting Bluetooth communications.

In another aspect, the present invention is directed to several embodiments of a method for detecting Bluetooth communications.

## BRIEF DESCRIPTION OF THE DRAWINGS

For a more detailed understanding of the invention, for further objects and advantages thereof, reference can now be made to the following description, taken in conjunction with the accompanying drawings, in which:

Figure 1 is a flow chart illustrating the set-up of a connection using Bluetooth, as known in the prior art;

Figure 2 is a block diagram showing a monitoring device in accordance with the present invention;

Figure 3 is a flow chart illustrating the method for detecting Bluetooth

communications according to the invention; and

Figure 4 is a flow chart illustrating complementary steps to the method of Figure 3.

## DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

In order to facilitate understanding of the invention, it will first be shown, as a specific example of Bluetooth communication, how a virtual serial port connection is set up between two devices using Bluetooth technology, as it is known to those skilled in the art. It should be understood however, that the invention is not limited to detection of virtual serial port connections.

FIG. 1 is a flow chart illustrating, in a slightly simplified way, the set up of the above-mentioned virtual serial port connection, in accordance with the prior art. The set up starts when a device comprising Bluetooth communication equipment (hereinafter referred to as the initiator) performs a so-called INQUIRY; step **102**. This INQUIRY can be said to page the surroundings, asking if there are any active Bluetooth devices within range. The INQUIRY comprises information about the class of service that is requested. In step **104** all such devices that are active and within range respond to the INQUIRY, by sending a Response message. This Response message comprises the device address of the responding device. The initiator – in this case the device or the user - then goes through the responses received in step **104** and chooses the device to communicate with; step **106**.

In step **108,** "PAGE" the initiator synchronises with the chosen responder. As Bluetooth is a spread-spectrum frequency hopping technology, it is vital to synchronise the transmission hopping frequency and clocks of the devices. The initiator initiates synchronisation with a PAGE message, comprising information about the chosen device. This device responds with a PAGE Response after which the initiator sends a Frequency Hop Synchronisation (FHS) message that

comprises the Bluetooth device address, i.e. the identity, and the clock of the initiator.

The initiator also creates a baseband ACL (Asynchronous ConnectionLess) connection; step **110**. This baseband can be seen as the base on which all the later communication will be built.

The initiator device then uses SDP (Service Discovery Protocol) to retrieve details of the responder and its serial port; step **112**. The RFCOMM(Radio Frequency COMM, a Bluetooth radio emulation of a COMM port well known in the art) server channel number is of particular interest. At this stage, the Service Name information may be presented to the user for verification.

With the Service Name information, the initiator then creates a L2CAP (Logical Link Control and Adaptation Protocol) channel that adapts upper layer protocols over the baseband. In addition, it establishes an RFCOMM connection over L2CAP; step **114**.

In step **116**, either device may then request that PAIRING be performed, which requires the use of a shared secret PIN code. Either device may also request that the baseband link be encrypted. No encryption is used before this step.

Finally, in step **118**, legacy application software is able to communicate through the virtual serial port, an example being synchronisation between a computer and a personal digital assistant (PDA).

Knowing how a connection is set up, it is time to discuss how to monitor unauthorised communication. As discussed earlier, Bluetooth uses spread-spectrum, frequency hopping and possibly encryption, making it very difficult or impossible to monitor on-going communication between Bluetooth devices. For the same reason, it is also very difficult to jam communication between Bluetooth devices.

On the other hand, INQUIRY, Response and PAGE messages are sent "in the clear" – i.e. prior to the establishment of the encryption procedures - making it

easy to track them. Referring now to Figure 2 that shows a block diagram of a monitoring device in accordance with the present invention. The monitoring device **20** comprises an antenna part **22**, a processor **24**, a memory **26** and a device for giving an alarm, advantageously a display **28**.

The antenna part **22** is advantageously tuned to receive all possible Bluetooth carriers - these are fixed and predetermined – but it would work, albeit not as efficiently, tuned to receive just one or some of the carriers. In order to improve the reception characteristics, some kind of diversity technique, usually space diversity, can be employed. In such a case, the antenna part **22** could comprise more than one antenna.

The processor **24** receives and listens to the signals received by the antenna part **22**. As soon as it detects evidence of a Bluetooth transaction, as an INQUIRY, PAGE, Response or FHS message, it gives an alarm that Bluetooth communication has been initiated. Said alarm could for instance be displayed on the display **28,** showing information about the transaction. In addition, the processor **24** can store information about the transactions in a memory **26**. Said information could be a time stamp, terminal identity and other relevant, available communication parameters. The terminal identity is not given in the INQUIRY message, while information about the requested service is, but all Response messages contain information about the identity. The information shown in the display **28** and stored in the memory **26** need not necessarily be the same.

A description of the method associated with the above-mentioned will now follow. The monitoring device **20** listens to all possible Bluetooth carriers, waiting for evidence of Bluetooth transactions. This usually comes in the form of an INQUIRY, PAGE, Response or FHS message; step **202**. When the device **20** detects something of interest, i.e. evidence of Bluetooth communication, it gives the alarm, step **204**, and logs information about the transaction, step **206**, after which it reverts to step **202**.

The monitoring device **20** is advantageously capable of simultaneously detecting and handling several different Bluetooth transactions. One way of doing this is for the method to be waiting for evidence (step 202) at all times and as soon as some evidence is found, deal with it in the appropriate way as described above. That is to say that while the monitoring device **20** is in the process of, for instance, giving the alarm (step **204**) it is at the same time listening for other transactions (step **202**).

It is not absolutely necessary for the method to comprise all of above-mentioned steps. For instance, the method could comprise step **202** and only one of the steps **204** and **206**.

The apparatus and the method described above could also comprise the complementary feature (to the apparatus) and the complementary step (to the method) of actively searching for Bluetooth equipment.

In this case, the detector device **20** further comprises means, usually software executed by the processor **24**. Said software orders the antenna part **22** to send regular INQUIRY messages and to listen for the Responses. As all Bluetooth equipment within range sends a Response, including equipment identity, upon reception of the INQUIRY, all Bluetooth equipment within range is easily detected and data about them are logged. If desired, said software could also possess the means to establish a connection with the Responding device and transmit a request to switch off all Bluetooth communication capabilities.

FIG. 4 shows the complementary steps of the method. These complementary steps comprise sending INQUIRY messages (step **210**) and listening to and logging Responses sent in reply to the INQUIRY message (step **212**). In addition, as shown in the figure, the complementary steps to the method could further comprise the step of setting up a connection with the equipment that sent Responses, requiring them to disable their Bluetooth connection capabilities (step **214**).

Although several preferred embodiments of the method and system of the present invention have been illustrated in the accompanying Drawings and described in the foregoing Detailed Description, it will be understood that the invention is not limited to the embodiments disclosed, but is capable of numerous rearrangements, modifications and substitutions without departing from the spirit of the invention as set forth and defined by the following claims.

**What is claimed is:**

1. An apparatus (20) for detection of Bluetooth transactions comprising:

an antenna part (22), the antenna part being tuned to receive signals of at least one Bluetooth carrier; and

a processor (24) listening to the signals received by the antenna part (22) and detecting evidence of a Bluetooth transaction.

2. The apparatus according to claim 1 further comprising a device for giving alarms (28) upon detection of evidence of a Bluetooth transaction by the processor (24).

3. The apparatus according to claim 1 where the evidence of a Bluetooth transaction is an INQUIRY message.

4. The apparatus according to claim 1 where the evidence of a Bluetooth transaction is a PAGE message.

5. The apparatus according to claim 1 where the evidence of a Bluetooth transaction is a Response message.

6. The apparatus according to claim 1 where the evidence of a Bluetooth transaction is an FHS message.

7. The apparatus according to claim 2 where the alarm device (28) is a display.

8. The apparatus according to claim 7 where the processor (24) displays information about the detected Bluetooth transaction in the display (28).

9. The apparatus according to claim 8 where the information is an identity of a transmitting terminal.

10. The apparatus according to claim 8 where the information is a time stamp.

11. The apparatus according to claim 1 further comprising a memory (26) in which the processor (24) stores information about detected Bluetooth transactions.

12. The apparatus according to claim 11 where the information is an identity of a transmitting terminal.

13. The apparatus according to claim 11 where the information is a time stamp.

14. The apparatus according to claim 1 where the antenna part (22) uses diversity techniques.

15. The apparatus according to claim 14 where the diversity technique is space diversity.

16. The apparatus according to claim 1 where the antenna part (22) is tuned to receive all Bluetooth carriers.

17. The apparatus according to claim 1 further comprising the means to send INQUIRY messages and to listen to and log the corresponding Responses.

18. The apparatus according to claim 17 further comprising the means to establish a connection with the device corresponding to each Response message, and to transmit a request to switch of the Bluetooth transmission capability.

19. A method for detection of Bluetooth transactions comprising steps of:

listening (202) to at least one Bluetooth carrier for detecting evidence of a Bluetooth transaction; and

taking appropriate action when evidence of the Bluetooth transaction is detected.

20. The method according to claim 19 where the evidence of Bluetooth communication is an INQUIRY message.

21. The method according to claim 19 where the evidence of Bluetooth communication is a PAGE message.

22. The method according to claim 19 where the evidence of Bluetooth communication is a Response message.

23. The method according to claim 19 where the evidence of Bluetooth communication is an FHS message.

24. The method according to claim 19 where the appropriate action is giving (204) an alarm.

25. The method according to claim 24 where the alarm is given on a display (28).

26. The method according to claim 25 where the display (28) shows information about a detected Bluetooth transaction.

27. The method according to claim 26 where the information is an identity of a transmitting terminal.

28. The method according to claim 26 where the information is a time stamp.

29. The method according to claim 19 where the appropriate action is logging (206) information about detected Bluetooth transactions in a memory (26).

30. The method according to claim 29 where the information is an identity of a transmitting terminal.

31. The method according to claim 29 where the information is a time stamp.

32. The method according to claim 19 further characterised in that it listens to all possible Bluetooth carriers.

33. The method according to claim 19 where the method returns to listening (202) after having taken appropriate action upon having detected a Bluetooth transaction.

34. The method according to claim 19 where the method is always listening (202) for evidence of Bluetooth transactions, while it is simultaneously able to perform other steps according to above-mentioned method.

35. The method according to claim 19 further comprising the complementary steps of:

sending (210) an INQUIRY message; and

listening to (212) and logging corresponding Responses.

36. The method according to claim 35 further comprising the step of setting up a connection to each device corresponding to said Responses and transmitting a request to switch off any Bluetooth communication capabilities (214).

5

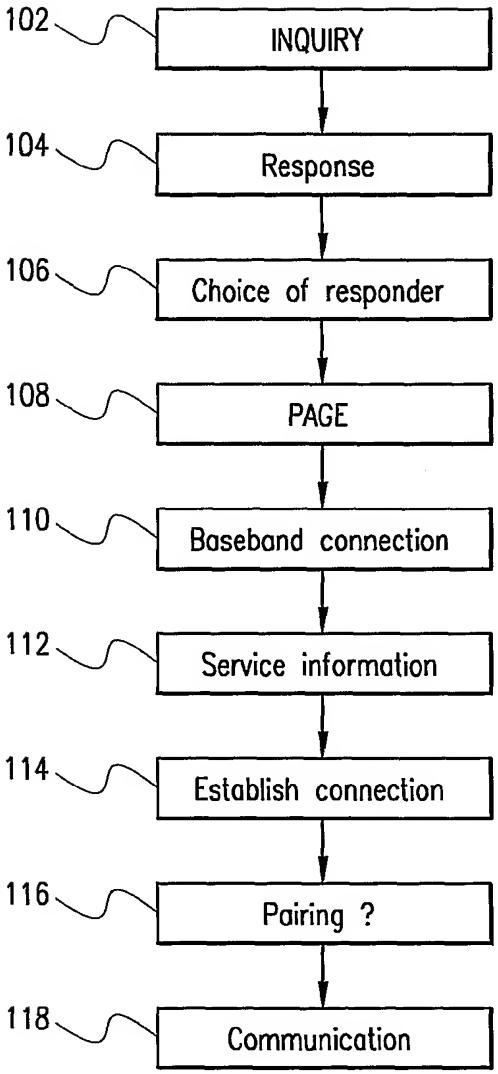



*FIG. 1*
(PRIOR ART)

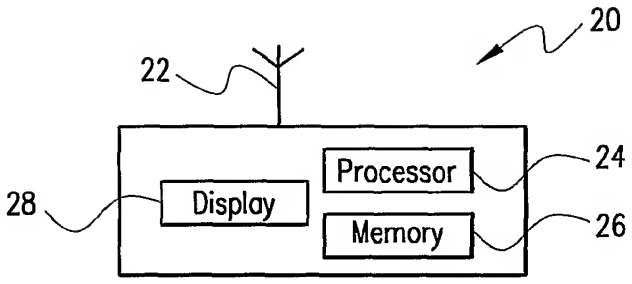



*FIG. 2*

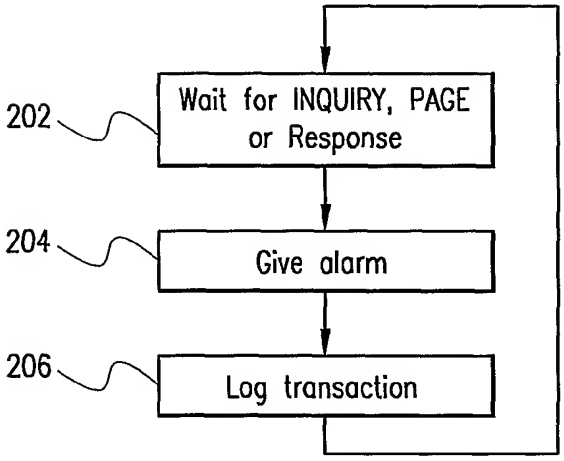



*FIG. 3*

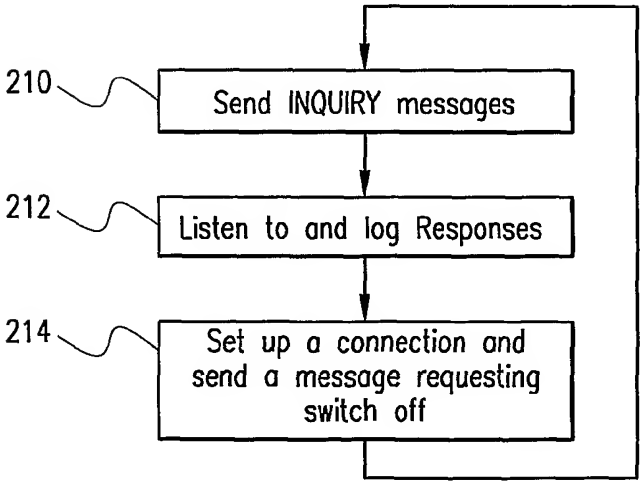



*FIG. 4*